IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application. No: 10/661,350	§		
Filed: September 12, 2003	§	Examiner:	Almeida, Devin E.
Inventor(s):	§	Group/Art Unit:	2132
Kay Hans-Peter Winkler,	§	Atty. Dkt. No:	5646-00900
Michael Ulrich Korner, Harald	§		
Ralf Schoning, Eckehard	§		
Hermann, Rene Kollmorgen,	§		
Dieter Hermann Kessler	§		
Title: SIGNATURE	§		
VALIDATION AND	§		
GENERATION	§		
	§		

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

Further to the Notice of Appeal mailed September 12, 2007, Appellants present this Appeal Brief. Appellants respectfully request that the Board of Patent Appeals and Interferences consider this appeal.

I. REAL PARTY IN INTEREST

The subject application is owned by Software AG, a corporation organized and existing under and by virtue of the laws of the Country of Germany, and now having its principal place of business at Uhlandstrasse 12, 64297 Darmstadt, Germany.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals.

III. STATUS OF CLAIMS

Claims 1, 3-12, 14-19, and 22-30 are pending in the case. Claims 2, 13, 20, and 21 were previously cancelled. All of the pending claims stand rejected and are the subject of this appeal. A copy of the claims, as incorporating entered amendments and as on appeal, is included in the Claims Appendix hereto.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the rejection in the Final Office Action of December 22, 2008. The Claims Appendix hereto reflects the current state of the claims.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Independent claim 1 relates to a method for validating a message with a signature. The method includes receiving the message with the signature. *See, e.g., at least page 2, line 27-page 3, line 6; page 5, lines 6-12; page 10, lines 7-16; page 11, lines 22-29; Figures 3-5.* The method further includes carrying out an integrated validation and storing process, which includes validation based on a validation algorithm and a key and storage of the message in a database. The integrated validation and storing process is performed within one atomic process, which prevents possible modification of the message between validation and storage. *See, e.g., at least page 3, line 7-11; page 3, line 22-page 4, line 21; page 4, line 28-page 5, line 29; page 10, lines 8-24; page 11, line 14-page 16, line 15; Figures 3 and 5.*

Independent claim 12 relates to a method for generating a signature for a message. The method includes carrying out an integrated receiving and generating process. The message is received and the signature is generated based on a signing algorithm and a key and is performed in an integrated manner, within one atomic process. Receiving the message and generating the signature within one atomic process prevents possible modification of the message between reception and generation of the signature. *See, e.g., at least page 6, line 1-page 7, line 20; page 11, line 4-13; Figure 4.* The method further includes sending the message with the signature. *See, e.g., at least page 7, lines 4-7 and 16-20; page 11, line 4-13; Figure 4.*

Independent claim 22 relates to an apparatus for validating a message with a signature. The apparatus includes first means for receiving a message with a signature. *See, e.g., at least page 2, line 27-page 3, line 6; page 5, lines 6-12; page 10, lines 7-16; page 11, lines 22-29; Figures 3-5, items 302, 305.* The apparatus further includes means for carrying out an integrated validation and storing process, which includes validation based on a validation algorithm and a key and storage of the message in a database. The integrated validation and storing process is performed within one atomic process, which prevents possible modification of the message between validation and storage. *See, e.g.,*

at least page 3, line 7-11; page 3, line 22-page 4, line 21; page 4, line 28-page 5, line 29; page 10, lines 8-24; page 11, line 14-page 16, line 15; Figures 3 and 5, item 305.

Independent claim 23 relates to an apparatus for generating a signature for a message. The apparatus includes a means for carrying out an integrated receiving and generating process. The message is received and the signature is generated based on a signing algorithm and a key and is performed in an integrated manner, within one atomic process. Receiving the message and generating the signature within one atomic process prevents possible modification of the message between reception and generation of the signature. *See, e.g., at least page 6, line 1-page 7, line 20; page 11, line 4-13; Figure 4, item 405.* The apparatus also includes a means for sending the message with the signature. *See, e.g., at least page 7, lines 4-7 and 16-20; page 11, line 4-13; Figure 4, item 405.*

Independent claim 24 relates to a method for validating a message with a signature. The method includes receiving the message with the signature. *See, e.g., at least page 2, line 27-page 3, line 6; page 5, lines 6-12; page 10, lines 7-16; page 11, lines 22-29; Figures 3-5.* The method further includes carrying out an integrated validation and storing process, which includes validation based on a validation algorithm and a key and storage of the message in a database. The integrated validation and storing process prevents possible modification of the message between validation and storage. *See, e.g., at least page 3, line 7-11; page 3, line 22-page 4, line 21; page 4, line 28-page 5, line 29; page 10, lines 8-24; page 11, line 14-page 16, line 15; Figures 3 and 5.*

Independent claim 28 relates to a method for generating a signature for a message. The method includes carrying out an integrated receiving and generating process. The message is received and the signature is generated based on a signing algorithm and a key and is performed in an integrated manner. Receiving the message and generating the signature in an integrated manner prevents possible modification of the message between reception and generation of the signature. *See, e.g., at least page 6, line 1-page 7, line 20; page 11, line 4-13; Figure 4.* The method further includes sending the message with

the signature. *See, e.g., at least page 7, lines 4-7 and 16-20; page 11, line 4-13; Figure 4.*

The summary above describes various examples and embodiments of the claimed subject matter; however, the claims are not necessarily limited to any of these examples and embodiments. The claims should be interpreted based on the wording of the respective claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 3, 4, 7, 8, 10, 12, 18, 19, 22-25, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis (WO 01/13574, "Kinnis") in view of Sarfati (U.S. Publication 2004/0015316, "Sarfati").

2. Claims 5, 6, 11, 14, 15, 17, 20, 21, 26, 27, 29, and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis in view of Sarfati and Slaughter (U.S. Patent 6,643,350, "Slaughter").

3. Claims 9 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis in view of Sarfati and Dickenson (U.S. Patent 6,853,988, "Dickenson").

VII. ARGUMENT

First Ground of Rejection

Claims 1, 3, 4, 7, 8, 10, 12, 18, 19, 22-25, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis (WO 01/13574, "Kinnis") in view of Sarfati (U.S. Publication 2004/0015316, "Sarfati"). Appellant respectfully traverses this rejection for the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 1, 4, 10, and 22

Regarding claim 1, Kinnis in view of Sarfati fails to disclose "carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database, and wherein said carrying out the integrated validation and storing process comprises storing said message and validating said signature within one atomic process". In the final rejection, the Office Action first relies on Kinnis for "wherein said carrying out the integrated validation and storing process comprises storing said message and validating said signature within one atomic process". More specifically, the Office Action cites page 16, lines 11-page 17, line 9 and page 15, lines 8-15 of Kinnis for the storing and validation step in general. Page 16, lines 11-19 describe validation of the certificate by valid date range and whether or not the certificate has been revoked. Page 16, line 20-page 17, line 9 describes decryption of the signature with a public key. If at any point the certificate is not verified or the decryption process fails, an error is generated and the process is halted. Page 15, lines 8-15 teaches that the digital signature service may verify the integrity of a document and, if it is verified, the document may be stored in a persistent store. Thus, Kinnis teaches verification and decryption as well as storage (upon successful verification) in a data store. Appellant notes that the process taught by Kinnis is substantially described in the background section of Appellant's own disclosure (see page 2) where prior art signatures may be use a key to generate a signature, validate the signature, and then store the signature. However, as noted on page 2 of Appellant's disclosure, this method has drawbacks, including the possibility of modification of the

message content between validation of the signature and further processing by the receiver.

Accordingly, Appellant is claiming a significant improvement over the teaching of Kinnis, whereby the validation and storing of the digital signature is performed as an integrated process. Appellant respectfully submits that Kinnis nowhere indicates that the validation and storage is an integrated process or is performed within one atomic process, which means that no modification can occur between validation and storage. Instead, Kinnis describes each of these steps separately and does not teach or suggest that the signature is validated based on a validation process and key and then stored in a database in an integrated process.

In response to these arguments, a previous Office Action (12/04/07) first states, "It is noted that the features upon which Appellant relies (i.e., where no modification can occur between validation and storage) are not recited in the rejected claim(s)." Appellant respectfully submits that the present claim recites that the validation and storage is an integrated process and occurs within one atomic process. It is clear from Appellant's specification that this feature has the advantage of protection from modification over Kinnis. Furthermore, as one skilled in the art understands, the use of the term "atomic process" in the claim clearly expresses how a possible modification of a message between validation and storage is prevented. The Office Actions in the present case have simply ignored the actual presented argument—that the process is integrated and occurs within one atomic process, which, as already submitted, is nowhere indicated in Kinnis.

The previous and most recent Office Actions assert:

> Kinnis teaches wherein in said integrated validation and storing process said message is stored and said signature is validated within one atomic process on page 15 lines 8-15 i.e. if the document is verified through the digital signature, the document and the signature are stored in a persistent data such as data store. [*Sic*]

Appellant has carefully reviewed the cited portion as well as the entirety of Kinnis and respectfully submits that there is **absolutely no** indication that the storage and validation of Kinnis is an integrated process which occurs within one atomic process. Instead, as already indicated, the cited portion teaches that the digital service may verify the integrity of a document, and then, if verified, store the document. Simply teaching

the individual steps of storage and corresponding validation amounts to nothing more than what is already identified in Appellant's own Background. In other words, there is no indication that Kinnis teaches anything other than the problem that the present Application addresses. As specifically required in the claims, the storage and validation steps must be integrated and occur within one atomic process. As already submitted, there is no teaching or suggestion of this feature in Kinnis, and furthermore, there is no occurrence of the terms "integrated" or "atomic process", much less any description ascribing these terms to validation and storage steps as required by claim 1.

Furthermore, Appellant notes that page 17, lines 6-7 of Kinnis states that after the previously described verification process is completed, the "recipient may process the document in any manner". There is no indication in this section of the necessity to store the document. Further, on page 3, lines 24-25, Kinnis states that the user may "store and/or transmit the document using any program for storing and transmitting files". Thus, in this case, Kinnis appears to **teach away** from the integrated process recited in the claims by stating that the document may be transmitted as an alternative to storing; clearly, if the document is not stored, but is transmitted, the validation storage process cannot be said to be "integrated" or occurring "within one atomic process". Additionally, Figure 8 of Kinnis illustrates a validation step, but makes no mention of storage in an integrated step or within an atomic process. The Examiner cannot simply assume that this feature is taught absent some teaching or suggestion otherwise from the prior art in any rejection.

Thus, both Kinnis and Sarfati fail to teach or suggest (and in fact, appear to teach away from) **carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database, and wherein said carrying out the integrated validation and storing process comprises storing said message and validating said signature within one atomic process**.

Furthermore, the combination of the references do not teach or suggest **wherein said storing said message and validating said signature within one atomic process prevents possible modification of the message between validation and storage**.

Appellant notes that the Office Action admits that "Kinnis does not teach where said message and validating said signature within one atomic process prevents possible modification of the message between validation and storage". More specifically, the Office Action relies on paragraph [0159] of Sarfati apparently for this feature of claim 1. However, the cited paragraph (and Sarfati in general) describes a receiver/decoder, which appears to be completely unrelated to the claimed features of claim 1. For example, paragraph [0159] recites:

> The engine 4008 comprises a code loader to load and download applications 4056 into the receiver/decoder memory. Only the necessary code is loaded into the RAM or FLASH memory, in order to ensure optimal memory use. The downloaded data is verified by an authentication mechanism to prevent any modification of an application 4056 or the execution of any unauthorized application. The engine 4008 further comprises a decompressor. As the application code (a form of intermediate code) is compressed for space saving and fast downloading from the MPEG stream or via a built-in receiver/decoder mode, the code must be decompressed before loading it into the RAM. The engine 4008 also comprises an interpreter to interpret the application code to update various variable values and determine status changes, and an error checker.

Thus, the cited portion describes a receiver/decoder which receives applications and verifies the downloaded data using an authentication mechanism. Appellant respectfully submits that this has nothing to do with carrying out an integrated validation and storing process, as specifically recited by the claims. Appellant notes that the Office Action apparently relies on this portion to "show the prevention of possible modification of the message between validation and storage" (see page 2 of the Final Office Action); however, paragraph [0159] states that the data is already stored in the memory at the time of verification, which does not at all prevent a possible modification between validation and storage because of the missing requirement of atomicity. Thus, the addition of Sarfati fails to address Appellant's claims or arguments and does not augment Kinnis at all. More specifically, as indicated above, neither reference teaches an integrated validation and storing process which occurs within one atomic process. As recited in the claim, performing this integrated storing and validation prevents possible modification of the message between validation and storage. Neither of the references is particularly relevant to this feature of claim 1. Thus, for at least the reasons provided above,

Appellant submits that Kinnis and Sarfati, alone or in combination, fail to teach all the features and limitations of claim 1.

Claim 3

Regarding claim 3, Kinnis in view of Sarfati fails to disclose "wherein the storing process is rolled back, if the signature is not valid". The Office Action relies on the storage of verified messages in a data store (page 15, lines 8-15) for this feature. However, Appellant respectfully submits that this section is completely irrelevant with respect to this feature of claim 3. Appellant notes that Kinnis teaches that an error is generated when the key is not valid or verified, but does not indicate that the storage process is rolled back. Correspondingly, Kinnis in view of Sarfati fails to disclose this feature of claim 3.

In response to these arguments, the previous Office Action asserts:

> Kinnis teaches wherein in said integrated validation and storing process said message is stored and said signature is validated within one atomic process on page 15 lines 8-15 i.e. if the document is not verified through the digital signature, the document and the signature are not stored in a persistent data store such as data store. [*Sic*]

Appellant first notes that the cited language occurs in previous claim 2 and is not recited in claim 3. Instead, claim 3 actually recites **wherein the storing process is rolled back, if the signature is not valid**. Appellant further notes that the provided sentence is actually not provided from Kinnis; instead, Kinnis states that if the document is verified, the document and the signature are stored in the persistent data store. This citation does not necessarily indicate the inverse statement as asserted by the Office Action, as one who is familiar with logic understands. Finally, Kinnis does not disclose what occurs if the signature is not valid.

Claims 7 and 8

Regarding claim 7, Kinnis in view of Sarfati fails to teach or suggest "wherein the integrated validation and storing process is carried out by said database". With respect to this feature, the Office Action relies on Figure 1, element 100 "Digital Signature Service"

and page 15, line 7-page 17, line 19. However, in these sections, the Digital Signature Service is nowhere described as a database. Additionally, the cited portion that the document and signature filed are stored in the data store 700 which appears to be a separate entity than the Digital Signature Service, which is in contradiction to the database of claim 1, where "said received message is stored" and which carries out "the integrated validation and storing process" (see claims 1 and 7). Thus, the Digital Signature Service of Kinnis fails to teach the database of claim 7.

Claims 12, 19 and 23

Regarding claim 12, Kinnis in view of Sarfati fails to teach or suggest "carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, and wherein said carrying out the integrated receiving and generating process comprises receiving said message to be sent and generating said signature within one atomic process". With respect to this feature, the Office Action relies on page 12, line 12 – page 15, line 5 of Kinnis. This section describes that a document and key may be retrieved from a data store, and that the signature may be generated. Similar to arguments above regarding claim 1, there is no indication that this is an integrated receiving and generating process which occurs within one atomic process. The Office Action further relies on the same paragraph of Sarfati as above. Appellant respectfully submits that the cited portions of Sarfati do not correspond to an integrated receiving and generating process as required by the claims. Instead, Sarfati relates to storage of an application and verification of that downloaded data. Thus, for at least the reasons provided above, Appellant submits that Kinnis in view of Safarti fails to teach all the features and limitations of claim 12.

Claim 18

Regarding claim 18, Kinnis in view of Sarfati fails to teach or suggest "wherein said integrated receiving and generation process is carried out in a database, where said message to be sent is stored". With respect to this feature, the Office Action relies on the same Digital Signature Service and citation as in claim 7 above. Similar to arguments

presented above regarding claim 7, the Digital Signature Service is nowhere described as a database and appears to be separate from the data store 700 where the document is stored. Accordingly, the Digital Signature Service of Kinnis fails to teach or suggest the database of claim 18.

Claim 24

Regarding claim 24, similar to arguments present above regarding claim 1, Kinnis in view of Sarfati fails to teach or suggest "carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database, and wherein said integrated validation and storing process prevents possible modification of the message between validation and storage".

Claim 25

Regarding claim 25, for at least the reasons provided above regarding claim 3, Kinnis in view of Sarfati fails to disclose "wherein the storing process is rolled back, if the signature is not valid".

Claim 28

Regarding claim 24, similar to arguments present above regarding claim 12, Kinnis in view of Sarfati fails to teach or suggest "carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, and wherein said carrying out the integrated receiving and generating process prevents possible modification of the message between said receiving and said generating".

Second Ground of Rejection

Claims 5, 6, 11, 14, 15, 17, 20, 21, 26, 27, 29, and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis in view of Sarfati and Slaughter (U.S. Patent

6,643,350, "Slaughter"). Appellant respectfully traverses this rejection for the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 5, 11, and 26

Regarding claim 5, Kinnis in view of Sarfati and Slaughter fails to teach or suggest "wherein said received message is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished". With respect to this feature, the Office Action relies on column 45, line 63-column 46, line 12 of Slaughter which generally relates to the nature of ACID transactions. As described in this section, Atomicity (the "A" in ACID) "means that a transaction should be done or undone completely". There is no indication in this section of a message that is received with a signature, and that prior to some integrated validation and storing process, the received message is locked, nor that it is released after such an integrated process. Thus, the cited portion simply defines ACID transactions and does not appear to relate to the recited feature at hand. Thus, Appellant respectfully submits that the mere definition of ACID transactions does not teach or suggest the specific feature recites in claim 5, nor does it provide an adequate reason to modify Kinnis and/or Sarfati to produce the features of claim 5. Correspondingly, the cited references fail to teach or suggest the features of claim 5.

Claims 6 and 27

Regarding claim 6, Kinnis in view of Sarfati and Slaughter fails to teach or suggest "wherein said received signature is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished". Similar to arguments provided regarding claim 5, the cited portions of Slaughter fail to relate to the locking of the received signature as recited in claim 6. Accordingly, the cited references fail to teach or suggest all the features of this claim.

Claims 14, 17, and 29

Regarding claim 14, Kinnis in view of Sarfati and Slaughter fails to teach or suggest "wherein said message to be sent is locked before the integrated receiving and generating

process is carried out and released after the integrated receiving and generating process has been finished". Similar to arguments provided regarding claim 5, the cited portions of Slaughter fail to relate to the locking of the message to be sent as recited in claim 14. Accordingly, the cited references fail to teach or suggest all the features of this claim.

Claims 15 and 30

Regarding claim 14, Kinnis in view of Sarfati and Slaughter fails to teach or suggest "wherein said key to be used for generating the signature is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished". Similar to arguments provided regarding claim 5, the cited portions of Slaughter fail to relate to the locking of the key to be used for generating the signature as recited in claim 15. Accordingly, the cited references fail to teach or suggest all the features of this claim.

Third Ground of Rejection

Claims 9 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kinnis in view of Sarfati and Dickenson (U.S. Patent 6,853,988, "Dickenson"). Appellant respectfully traverses this rejection for at least the reasons provided above regarding claims 1 and 12.

CONCLUSION

In light of the foregoing amendments and remarks, Appellant submits the application is now in condition for allowance, and an early notice to that effect is requested.

If any extensions of time (under 37 C.F.R. § 1.136) are necessary to prevent the above-referenced application(s) from becoming abandoned, Appellant(s) hereby petition for such extensions. The Commissioner is hereby authorized to charge any fees which may be required or credit any overpayment to Meyertons, Hood, Kivlin, Kowert & Goetzel P.C., Deposit Account No. 50-1505/5646-00900/JCH.

Respectfully submitted,

/Jeffrey C. Hood/

Jeffrey C. Hood, Reg. #35198
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert & Goetzel PC
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800
Date: 2009-06-17 JCH/JLS

VIII. CLAIMS APPENDIX

The following lists claims 1, 3-12, 14-19, and 22-30, incorporating entered amendments, as on appeal.

1. A method for validating a message with a signature, wherein said method comprises:

receiving said message with said signature; and

carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database, and wherein said carrying out the integrated validation and storing process comprises storing said message and validating said signature within one atomic process;

wherein said storing said message and validating said signature within one atomic process prevents possible modification of the message between validation and storage.

3. The method according to claim 1, wherein the storing process is rolled back, if the signature is not valid.

4. The method according to claim 1, wherein the storing process is completed, if the signature is valid.

5. The method according to claim 1, wherein said received message is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

6. The method according to claim 1, wherein said received signature is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

7. The method according to claim 1, wherein the integrated validation and storing process is carried out by said database.

8. The method according to claim 7, wherein the integrated validation and storing process is controlled by said database.

9. The method according to claim 1, wherein said message is an XML-document.

10. The method according to claim 1, wherein said signature is a digital signature.

11. The method according to claim 1, wherein said integrated validation and storing process is carried out as an ACID transaction.

12. A method for generating a signature for a message, wherein said method comprises:

carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, wherein said carrying out the integrated receiving and generating process comprises receiving said message to be sent and generating said signature within one atomic process, and wherein said receiving said message and said generating said signature within one atomic process prevents possible modification of the message between said receiving and said generating, and

sending said message with said signature.

14. The method according to claim 12, wherein said message to be sent is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

15. The method according to claim 12, wherein said key to be used for generating the signature is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

16. The method according to claim 12, wherein said message is an XML-document.

17. The method according to claim 12, wherein said integrated receiving and generating process is carried out as an ACID transaction.

18. The method according to claim 12, wherein said integrated receiving and generation process is carried out in a database, where said message to be sent is stored.

19. The method according to claim 12, wherein said signature is a digital signature.

22. An apparatus for validating a message with a signature, wherein said apparatus comprises:

a first means for receiving said message with said signature; and

a second means for carrying out an integrated validation and storing process, wherein said second means are capable and affected to validate said signature based on a validation algorithm and a key and to store said message, wherein said carrying out the integrated validation and storing process comprises storing said message and validating said signature within one atomic process, and wherein said storing said message and validating said signature within one atomic process prevents possible modification of the message between validation and storage.

23. An apparatus for generating a signature for a message, wherein said apparatus comprises:

means for carrying out an integrated receiving and generating process, wherein said means are capable and affected to receive said message to be sent and to generate said signature based on a signing algorithm and a key, wherein said carrying out the integrated receiving and generating process comprises receiving said message to be sent and generating said signature within one atomic process, and wherein said receiving said

message and said generating said signature within one atomic process prevents possible modification of the message between said receiving and said generating; and

means for sending said message with said signature.

24. A method for validating a message with a signature, wherein said method comprises:

receiving said message with said signature; and

carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database, and wherein said integrated validation and storing process prevents possible modification of the message between validation and storage.

25. The method according to claim 24, wherein the storing process is rolled back, if the signature is not valid.

26. The method according to claim 24, wherein said received message is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

27. The method according to claim 24, wherein said received signature is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

28. A method for generating a signature for a message, wherein said method comprises:

carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, and wherein said carrying out the integrated receiving and generating process prevents possible modification of the message between said receiving and said generating, and

sending said message with said signature.

29. The method according to claim 28, wherein said message to be sent is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

30. The method according to claim 28, wherein said key to be used for generating the signature is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131 or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no decisions on any related proceedings.